DTCP Volume 1
Supplement C
Mapping DTCP to Bluetooth (Informational Version)

Hitachi, Ltd
Intel Corporation
Matsushita Electric Industrial Co., Ltd.
Sony Corporation
Toshiba Corporation

Revision 1.0
April 26, 2004

DTLA Confidential

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Hitachi, Intel, MEI, Sony, and Toshiba (collectively, the “5C”) disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Some portions of this document, identified as "Draft" are in an intermediate draft form and are subject to change without notice. Adopters and other users of this Specification are cautioned these portions are preliminary, and that products based on it may not be interoperable with the final version or subsequent versions thereof.

Copyright © 1997 - 2004 by Hitachi, Ltd., Intel Corporation, Matsushita Electric Industrial Co., Ltd., Sony Corporation, and Toshiba Corporation (collectively, the “5C”). Third-party brands and names are the property of their respective owners.

Intellectual Property

Implementation of this specification requires a license from the Digital Transmission Licensing Administrator.

Contact Information

Feedback on this specification should be addressed to dtla-comment@dtcp.com.

The Digital Transmission Licensing Administrator can be contacted at dtla-manager@dtcp.com.

The URL for the Digital Transmission Licensing Administrator web site is: http://www.dtcp.com.

Table of Contents

Figures

Volume 1 Supplement C DTCP Mapping to Bluetooth

V1SC.1 Introduction

This supplement describes the mapping of DTCP onto the Bluetooth. All aspects of IEEE 1394 DTCP functionally are preserved and this supplement details Bluetooth DTCP specific changes or additions.

V1SC.1.1 Related Documents

This specification shall be used in conjunction with the following publications. When the publications are superceded by an approved revision, the revision shall apply.

- Digital Transmission Content Protection Specification
- Bluetooth SIG, Inc. specifications:
    - Audio/Video Distribution Transport Protocol Specification Revision 1.0
    - Bluetooth Assigned Numbers
    - Advanced Audio Distribution Profile
    - Generic Audio/Video Distribution Profile

V1SC.1.2 Terms and Abbreviations

AVDTP	Audio/Video Transport Layer Protocol Specification 1.0

V1SC.2 Modifications to Chapter 6 (Content Channel Management and Protection)

V1SC.2.1 Exchange Key Expiration

Sources of protected content expire their Exchange Keys when all AVDTP connections are released.

V1SC.2.2 Content Encryption Format

DTCP prefixes a one byte header to the Media payload and encrypts both and then again affixes another two byte header as shown in following figure.

	msb							lsb
Header[0]	EMI		Reserved (00_2)		Padding Length (0000_2-1111_2)			
Header[1]	Reserved(0000000_2)							Odd/ Even
EC[0]	Encrypted Header							
EC[1]	Protected Content(Media payload plus 0 to 15 bytes of padding)							
EC[2]								
-								
-								
-								
EC[N]								

Figure 1 Protected Content Packet

Header [0..1]: This field is used to carry the bits described in Sections 6.3.3 “Odd/Even Bit” and 6.4.2 “Encryption Mode Indicator (EMI)” and Padding Length which specifies the length of the padding affixed to Media payload.

EC[0]: The Encrypted Header (EH) consists of at least 1 byte and is used as depicted in following

	msb							lsb
EC[0]	reserved zero							CT

Figure 2 Encrypted Header

CT (Content Type): specifies the treatment of EMI/Embedded CCI for the Media Payload in the PCP and the value of which are described in following table:

CT	Definition	Meaning
0_2	Audiovisual Content	Rules for audiovisual device functions described in Section 6.4.4 are applied
1_2	Audio Content	Rules for audio device functions described in Section 6.4.5 are applied

Table 1 Content Type

EC[1..N]: is the encrypted form of the Media payload with padding.

When M6 is used to protect payload it can range from 7 to 65520 bytes in length and padding is affixed when payload length is less than 7 bytes.

When AES-128 is used to protect payload it can range from 15 to 65520 bytes in length and padding is affixed when payload length is less than 15 bytes.

V1SC.3 Embedded CCI

Embedded CCI is carried as part of the content stream. Many content formats including MPEG have fields allocated for carrying the CCI associated with the stream. The definition and format of the CCI is specific to each content format. Information used to recognize the content format should be embedded within the content.

V1SC.4 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions)

V1SC.4.1 Control Packet Format

This section maps the AKE control command specified in Section 8.3.1 to the Bluetooth AVDTP_SECURITY_CONTROL_CMD and AVDTP_SECURITY_CONTROL_RSP. The AKE control command sub fields used with Bluetooth have the same values and functions as detailed in Chapter 8.

	msb							lsb
Control[0]	reserved (zero)				ctype/response			
Control[1]	category – 0000_2 (AKE)				AKE_ID			
Control[2]	subfunction							
Control[3]	AKE_Procedure							
Control[4]	exchange_key							
Control[5]	subfunction_dependent							
Control[6]	AKE_Label							
Control[7]	number				status			
Control[8]	Byte Length N of AKE_Info Field							
Control[9]								
AKE_Info[1]	AKE_Info							
- -								
AKE_Info[N]								

Figure 3 Bluetooth DTCP Control Packet Format

- Control bytes 0, 8, and 9 are used to map DTCP to Bluetooth.
- Ctype has the same values as referenced in chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command Set.
- Control bytes 1..7 are identical to operand bytes 0..6 as specified in section 8.3.1.
- The AKE_Info field is identical to the data field specified in section 8.3.1.

V1SC.4.2 Status Packet Format

This section maps the AKE status command specified in Section 8.3.2 to the Bluetooth AVDTP_SECURITY_CONTROL_CMD and AVDTP_SECURITY_CONTROL_RSP. The AKE status command sub fields used with Bluetooth have the same values and functions as detailed in Chapter 8.

	msb							lsb
Control[0]	reserved (zero)				ctype/response			
Control[1]	category = 0000_2 (AKE)				AKE_ID = 0000_2			
Control[2]	subfunction							
Control[3]	AKE_Procedure							
Control[4]	exchange_key							
Control[5]	subfunction_dependent							
Control[6]	AKE_Label = FF_{16}							
Control[7]	number = F_{16}				status			

Figure 4 Status Packet Format

- Control byte 0 is used to map DTCP to Bluetooth.
- Ctype has the same values as referenced in Chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command Set.
- Control bytes 1..7 are identical to operand bytes 0..6 as specified in Section 8.3.2.
- The maximum data field query supported by exchanging values via the **data_length** field and described in the last paragraph of section 8.3.2 is not needed, as it is supported low level AVDTP.

V1SC.4.3 CONTENT_KEY_REQ subfunction

In section 8.3.4.6, isochronous_channel_number field is replaced with the ACP SEID value.

V1SC.5 Bluetooth Information (Informative)

AVDTP provides for content protection capability identification and configuration via CP_TYPE[1] which for DTCP CP_TYPE is 0001_{16}..

[1] Bluetooth SIG, Bluetooth Assigned Numbers, http://www.bluetooth.org/foundry/assignnumb/document/assigned numbers